Information Management: Is the U.S. Army prepared for Information Superiority?

A Monograph
by
MAJOR Timothy P. Norton
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
AY 02-03

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

MAJOR Timothy P. Norton

Title of Monograph: Information Management; Is the U.S. Army prepared for Information Superiority?

Approved by:

_____	Monograph Director
LTC Jeffrey R. Witsken, MMAS	
_____	Professor and Director Academic Affairs, School of Advanced Military Studies
Robert H. Berlin, Ph.D.	
_____	Director, Graduate Degree Program
Philip J. Brookes, Ph.D.	

Abstract

Information Management; Are we prepared for information superiority? by Major Timothy P. Norton, U.S. Army, 49 pages.

Although the Army Vision 2010 states that one of the keys to success on the modern battlefield is to achieve information superiority, the current U.S. Army doctrine in this area does not support it. Specifically, the topic of information management, one of the fundamentals in information superiority, is lacking in the clarity and depth required to meet this lofty goal.

Operational advantages of information superiority are obtained through the systematic provision of clear, accurate, and useable information. Under the current doctrine, the discussion is limited to the products and ignores the process. If a product focus is not addressed the U.S. Army will not reach the stated goal of information superiority.

To understand this serious deficiency, this study examines current doctrinal definitions and concepts of information management and compared them with business and academic writings on the subject. The intent was to assess if the Army's concepts are sufficient to manage the information that we strive to create.

The researched revealed that the Army is not prepared. Doctrine does not provide guidance on the concept of information management as a system. The doctrinal definitions identify products and qualities of information but fail to discuss frameworks and principles that are essential to information management. This gap in information management doctrine makes it nearly impossible to achieve the goal of information superiority.

The Army must address these weaknesses in current doctrine. To improve information management, the Army must redefine the term information management in a manner that supports a systems approach, produce a conceptual framework for its application, publish principles of information management, and produce a single source document for information management doctrine.

Table of Contents

Table of Contents 1
Figures 1
Tables 1
Introduction 1
Methodology 3
Criteria 4
Structure 7
Information Management – Doctrinal View 9
Understanding Information Superiority Goals 9
Understanding Doctrinal Information Management 14
Information Management – A System View 20
Redefining Information 20
Redefining Management 25
Information Management – A constitutional framework 27
Principles of Information Management 35
Conclusions and Recommendations 41
Conclusions 42
Recommendations 43
Bibliography 47

Figures

Figure Page

1. Information Superiority Model 12
2. CG-CC-CR-CV Analysis 13
3. Cognitive Hierarchy 16
4. Constitutional Model 31
5. An Army Example 32
6. Principles of Information Management 36

Tables

Table Page

1. Types of Information Value 24

CHAPTER ONE

Introduction

> "…if a commander's service of information is better than that of his adversary he possesses wider knowledge and superior control; he selects with certainty his objective and arrives first; he perceives weaknesses before his own is discovered or strength before his weakness is known; he anticipates movements, alters dispositions, executes plans unknown to his enemy; in short, the successful soldier commands the situation by force of superior knowledge, and never is it more true than in war knowledge is power. The commander inferior to his enemy in character and service of his intelligence communication is like a blind man fighting him who can see. It follows that his information service must be the best, and also that he must use it to his fullest extent."[1]
>
> BG George P. Scriven, Chief Signal Officer of the Army, 1915

The Army Vision 2010 outlines key tenets for achieving dominance on the modern battlefield. One of the tenets is information superiority. The vision of information superiority emphasizes the ability to collect, process, and disseminate information in a seamless fashion. For this reason, the quote from BG Scriven is a perfect way to begin the examination of information management. The Army that Scriven describes is one that has only recently begun to grasp the power of the telegraph and exploit it for all its capabilities, yet clearly understood is the power of information on the battlefield. In a similar fashion, the U.S. Army of 2003 has only scratched the surface of the powerful technologies available. The modern day Army is faced with the similar problems of Scriven's Army and wishes to achieve the same goals. This goal manifests itself in Scriven's statement in the final sentence," use (information) it to its fullest".

Scriven points out that the key to success on a battlefield is not merely gaining the best information possible and but the exploitation of it to its maximum use. The U.S. Army has

[1] George P. Scriven, *Service of Information, United States Army* (Washington DC: Government Printing Office, 1915), 14.

tremendous means to gather and distribute information. It is on the leading edge in leveraging information technology in military operations. Unfortunately, information "en masse" is not knowledge. Although a simple concept, this blinding flash of the obvious is a key factor to success. Knowledge includes providing the correct, analyzed, and timely information to decision makers in a usable format. More succinctly stated it is the proper management of information.

Information management has a profound affect on concepts and capabilities at the operational and tactical level. It is fundamental in the planning and decision-making processes. Information that a commander does or does not have drives decisions. It is central to visualizing his battlespace.[2] Additionally, information assists commanders in overcoming and managing uncertainty. FM 6.0 states that there four sources of "fog" that must be overcome and all four are information related.[3]. Therefore, the need for information on the battlefield is essential to commanders and yet it is a source of fog. What then is the solution? This paper will argue that the solution is proper information management.

This monograph asks; is the U.S. Army prepared to manage the information created on the modern battlefield? Although straightforward in the asking, the answer is undoubtedly much more complex. Answering this question is more than just an analysis of FM 3.0's definition of information management, or a look at the complex hardware and software platforms in development. It is asking ourselves if we have developed a theoretical model that assists in framing the information environment in which we operate. Simply put, is the Army prepared to handle the information superiority that we strive to achieve?

---

[2] Headquarters, Department of the Army, *FM 6.0 Command and Control* DRAG (Washington DC, Government Printing Office, TBP) 4-6 – 4-7. This reference describes the visualization process through the gathering of CCIR, EEFI, and FFIR (information) which then follows an information hierarchy towards situation understanding.

[3] *FM 6.0*, 4-4. The sources of fog are: inadequate information, misinterpretations of information, conflicting information, and too much information.

Methodology

This monograph is concerned with doctrinal definitions and concepts as they support the commander in the overall goal of information management. It is an examination of the current U.S. Army doctrine on Information Management. The evaluation technique used in this monograph is to avoid the technical aspects of information management and focus on the conceptual framework required to create a usable system. There are a couple of benefits in adopting this methodology. This methodology provides the greatest flexibility for use in the ever-changing technology environment. The findings and recommendations are not constrained by changing software or machines but rather reliant on the processes and principles required to manage information. More importantly, the greatest benefit in focusing on concepts is that it best supports the ultimate goal of information management – gaining operational advantages.

To accomplish this goal, the research question has two main components. The first component was information superiority. An examination of information superiority provides a greater understanding of the goals and objectives of information use within the Army. This examination required the use of two models. The first model is Carl Von Clausewitz's center of gravity model.[4] This model establishes the need to evaluate an item for the source of its power. Although useful, in order to examine the center of gravity more in-depth an additional analysis was required. A professor with the Marine Corps University, Dr. Joe Strange's[5] provides a monograph with such a model. His theory, in application, assesses the dangers and opportunities of a center of gravity. The application of these two theories allowed a focus on a vulnerability of

[4] Carl Von Clausewitz, *On War*, trans and eds, Michael Howard and Peter Paret, indexed edition, (Princeton, New Jersey: Princeton University Press, 1984), 595.

[5] Joseph Strange, "Centers of Gravity and Critical Vulnerabilities" *Perspectives on Warfighting*, (Number 4, Second Edition 1996).

information superiority – management of information. Additionally, it demonstrated the importance and criticality of information management. .

These models enabled the logical progression to the examination of the second component – information management. After establishing information managements' importance, an investigation into the doctrinal definition and use was required. This assessment provides a common understanding and vocabulary for the monograph. Two field manuals, FM 3.0 Operations and FM 6.0 Command and Control, accomplished these tasks. Their use establishes the requirement for military forces to gain and maintain information superiority, thus properly manage information. In short, both of the field manuals stress the need for relevant information as a key to gaining information superiority.

Once the analysis of definitions and processes were completed, a measurement tool was required to assess there utility. Business and academic writings provided these tools. Applicable business concepts provide a depth understanding information management that was not contained in current doctrine. These included; operational frameworks, processes and structure. By comparing these concepts to Army doctrine, fundamental principles and frameworks of information management became visible. The combination of these ideas provided four distinct, yet interrelated, criteria that form the body of this paper.

Criteria

The criteria used in evaluating Army doctrinal concepts for information management all revolve around one main theme – systems versus products. Each of these criteria evaluates a portion of the doctrine to identify if there is a developing system of information management or merely product focus on information requirements. They are all inter-related and build upon one another.

The initial criterion current doctrine must meet is to provide a definition of information management. This measure has two parts. The first is the definition for information. Academic writings provide several ways to define information and this paper evaluates them against the Army's current definition. The next aspect of this criterion is a definition of management. A discussion of the classic functions of management provides a tool to analyze information management within Army doctrine. The important goal of this criterion is to establish whether Army doctrine identifies information management as a product or a system. The recognition of this drives the remainder of information thought processes. A systems approach in managing information is the most favored by business and academic writings. The argument states that if the "system" method is foregone for a "product" method then information management does not truly exist. The understanding of which method the Army embraces is essential in establishing the relevancy of the remaining criteria.

The next criterion asks if current doctrine provides a framework that underlines its definition of information management. A framework must encompass the definitions as well as provide a tool for use in Army operations. Once established, the framework is then matched against a supporting criterion; principles of information management. This is simply a search for the Army principles for developing an information management plan. This criterion nests itself in the time-tested use of the principles of war to assist in the planning of military operations. Principles are not checklists; however, they do provide a common thought process for establishing sound plans. Information management planning requires similar principles.

Theses criteria all lead to the last measure; the overall organization of information management doctrine. Does information management doctrine have the requisite clarity, depth, and organization? The research has demonstrated that the need to gain and maintain information superiority is without question. Each of its parts is equally critical to the success of the Army on the modern battlefield. Information operations (IO) and intelligence, surveillance, and

reconnaissance (ISR) enjoy a large body of military writings but noticeably lacking is the same breadth of writing on information management. Yet this area is as critical to information superiority as the other two. Because of this linkage, this criterion is essential. It asks if the doctrine has structured this subject in a usable and easy to find manner. This criterion speaks directly to clarity and usability. Does doctrine arrange the subject in an orderly, understandable, and useful format? Finally, it suggests that doctrine cannot ignore this subject if the Army wishes to achieve information superiority.

An element of importance for this monograph is its limitations. These limitations allow for a focus on the he theoretical and conceptual process of information management. Through this a conceptual understanding of information management is achieved. For that reason, this monograph does not address technology. It is the author's opinion that technology is a tool to manage information but it is not information management. A focus on technology would distract the reader from true strength of information management – the system[6]. Additionally, this paper is not a guide to developing an information management plan. The goal is to establish if doctrine meets the general requirements of describing information management. Information management plans are very specific and more often than not unit related. Lastly, this paper does not address critical vulnerabilities within information superiority that are outside the realm of information management. IO and ISR both have vulnerabilities and are worthy topics. Nevertheless, time and space preclude a discussion on them. It is for that reason that this paper focuses on information management vulnerabilities.

[6] Multiple articles and books stressed this point. A summarization of them is that the amount of technology used in information management does not translate directly into success. For more information on this argument see: Morton F. Meltzer, *Information: the ultimate management resource,* (New York: AMACOM, 1981), 9; Nancy Ferris, "Knowledge is power, Really." (Government Executive, June 1999), 63-64; Martin Van Creveld, *Technology and War- From 2000 B.C. to the present.* (New York: The Free Press, 1989), 247; and Anthony Garrett, "Information Superiority and the future of mission orders." (Military Review, November-December 1999), 61-69.

Structure

To accomplish the task of discussing the criteria the monograph is broken into several parts. The initial discussion within the document evaluates the current doctrinal definitions and descriptions. This section sets the foundation for further development of information management as a concept. It begins by providing an analysis of information superiority, which then developed into a set of vulnerabilities. These vulnerabilities are the "product" driven information management vice a system or framework. The major emphasis in this section is to provide a coherent understanding of the strengths and weaknesses within our current doctrine measured against the criteria. The goal of this section is to provide the reader with a clear understanding of the importance of information management. It also establishes the weaknesses within current doctrine. The weakness address set the stage for the next section.

The next section addresses the vulnerabilities brought forward in the initial discussion of information superiority. By measuring doctrine against the criteria identified earlier (the definition of information management, a framework for the process, and principles for implementation of information management) along with business models and academic writings, concepts and principles are developed for consideration. Current doctrinal strengths coupled with these models result in practical solutions to some of the issues. The outcome is the foundation for the final section.

The final section of the monograph provides conclusions and recommendations for inclusion in current and future Army doctrine. The linkage between the four criteria and current doctrine are solidified within this section. Finally, this section provides a framework for understanding information management as a system and not just products.

The structure outlined above provide a path to understanding information management as process. This paper argues that taking a systems approach in managing information the goal of producing timely, accurate, relevant, and useable information is achievable. If ignored for a

"product" method then the decision-making cycle eventually deteriorates and advantages of information superiority are lost.

Finally, this paper accepts the fact that information superiority is essential today and will continue to be in the future for operational success. The intent is to provide an analysis of information management that demonstrates a critical vulnerability in our doctrinal definitions and ambitions. The investigation of current doctrine demonstrates that without completely understanding and establishing a framework for what we wish to achieve, we may add to the fog and friction in the information battlefield. More clearly stated; if we wish to handle the information created on the modern battlefield we must establish a solid doctrinal understanding of information management.

CHAPTER TWO

Information Management – Doctrinal View

Understanding Information Superiority Goals

The evaluation of the current doctrinal definitions and descriptions of information management are the focal point within this chapter. This discussion sets the groundwork for further development of information management as a system. The evaluation begins by providing an analysis of information superiority, focusing on its vulnerabilities. The major emphasis in this section is to provide a coherent understanding of the strengths and weaknesses within our current doctrine measured against the four criteria. The goal of this section is to provide the reader with a clear understanding of the importance of information management and establish the weaknesses of it within current doctrine.

Before a discussion on information management can take place, a common understanding of its derivative and importance must be established. To accomplish this goal, an analysis of information superiority is required. This provides the intellectual framework for further discussions of opportunities and threats within this tenet of Army Vision 2010.

The amount of information available today is greater than at any time in history and for the near future it will continue to grow exponentially. A much-quoted remark is that a weekday copy of the New York Times has more information than the average person in the 17th Century England would see in an entire lifetime.[7] Although the quote is anecdotal at best, there is no doubt that the speed of information flow has increased dramatically. Moore's law[8] tell states that

[7] Shirley Douglin Kennedy, "Finding a cure for information anxiety", *Information Today (MAY 2001) 40-41*

[8] The observation made in 1965 by Gordon Moore, co-founder of Intel that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the near future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months, and this is the current

the speed of processors for computers double every 18 months, hundreds of television channels are available, wireless technology is on the rise, and the internet has become the main source of information for many Americans.

There is however a counter-argument against this "perceived" information windfall. Arguments exist stating there has always been as much information available as humans could process. The fear of getting overwhelmed is not from the information available but rather from inability to understand or make it available for a positive use (decisions). Oddly enough, similar concerns arose when the printing press was invented.[9] No matter which side is "correct", the military has recognized this information explosion. Although an RMA debate rages, the fact remains that the environment the Army operates in today is fundamentally different from that of 60 years ago. A battalion commander during World War II was ill informed about the world outside of his area of operations. Soldiers in Vietnam could not "chat" with spouses at home via AOL Chat rooms. The instantaneous communications available to the military have become both a blessing and a curse. The blessing is that information is immediately available (theoretically) and the curse is that *information is immediately available.* An engagement on the modern battlefield that broadcasted back to a waiting audience results in possible strategic implications.

The military has recognized this and has added the information environment to the battle space of a commander. The doctrinal definition of the information environment is the "aggregate of individuals, organizations, or systems that collect, process, or disseminate the information; and also includes the information itself."[10] A key to this concept is the recognition that most of the "environment" it is not within the control of the commander. This being said it still is necessary

---

definition of Moore's Law, which Moore himself has blessed. Most experts, including Moore himself, expect Moore's Law to hold for at least another two decades.

[9] Bruce, Bertram C and Bernard Junwirth, "Information Overload: Threat or Opportunity?" *Journal ofAdolescent &Adult,* (February 2002) 400-406

[10] Headquarters, Department of the Army, *FM 3.0 Operations* (Washington DC, Government Printing Office, 2001),1-4. Hereafter *FM 3.0*

to dominate it. The manner in which the military dominates this environment is through information superiority.

Army Field Manual 3.0 defines information superiority as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying the adversary's ability to do the same."[11] The operational advantages sought are better and faster decisions, a degradation in the enemy's decision cycle, and an impact on the enemy and others perceptions of the military and its operations. Additionally, the Army stresses the qualitative nature of information as one of the key tenets required to conduct decisive operations.[12] Joint Publication 3.0 has similar definition but noticeably absent is the term "operational advantage". The Joint definition focuses more on the capability rather than goal of superiority.[13]

To achieve an operational advantage from information superiority, FM 3.0 provides three interrelated activities; intelligence, surveillance, reconnaissance (ISR), information management, and information operations. Figure 1 – Information Superiority, demonstrates the Army understanding of these processes.

The diagram attempts to highlight the integration of these actions resulting in the operational advantages discussed earlier. Using the information superiority definition as a guide to the model; collection would be found in ISR and IO, the processing within information management, and dissemination would then flow back through ISR and IO.

---

[11] *FM 3.0, 11-2*

[12] *FM 3.0,* 11-2.

[13] Department of Defense, *Joint Publication 3.0, Operation* (Washington DC: GPO, 2001) 172. defines IS as The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. It should be noted that JP 6.0 C4I does not have the term information superiority within its text.

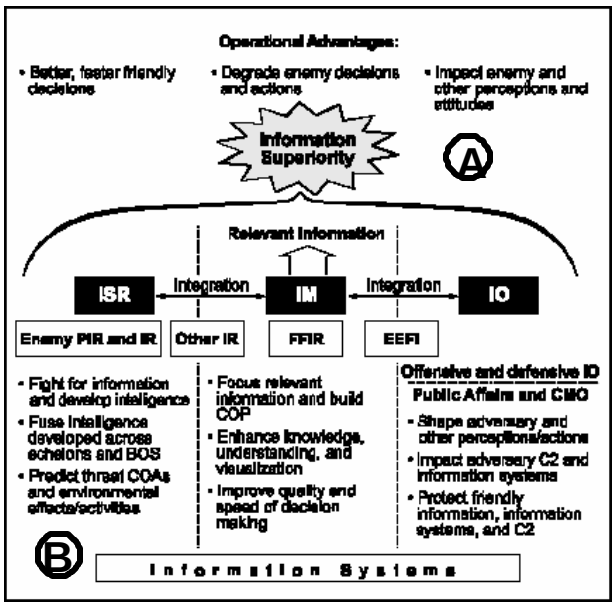


Figure 1 -Information Superiority

Source: Headquarters, Department of the Army,*Field Manual No 3.0 Operations* (Washington, D.C: Government Printing Office, 2001) 11 -2

The result is information superiority or more specifically, operational advantages. If the overall intent of information superiority is to achieve an advantage then an analysis of the doctrinal process should provide a means that clearly points in that direction. Dr. Joe Strange provides a good tool for this analysis.

Dr. Strange asserted in his monograph that the U.S. Military, as a community, does not speak a common language when referring to Carl Von Clausewitz's center of gravity theory.[14] Strange's monograph highlights the differences in each services definitions and he offers his own. Additionally, he provides an analytical tool to direct energy at the center of gravity. Strange's

[14] *On War*, 595-6. Clausewitz defines "center of gravity (as) the hub of all power and movement, on which everything depends. It is the point at which all our energies should be directed."

definition is simply the "primary sources of moral or physical strength, power and resistance."[15] The definition supports his further statements regarding critical capabilities, critical requirements, and finally critical vulnerabilities. Because the Strange's model illuminates vulnerabilities, it is a good tool for examining information superiority.

Figure 2 provides an analysis of Information superiority using this model and overlaying it with the contents of Figure 1. In this model, the center of gravity identified is information superiority[16].

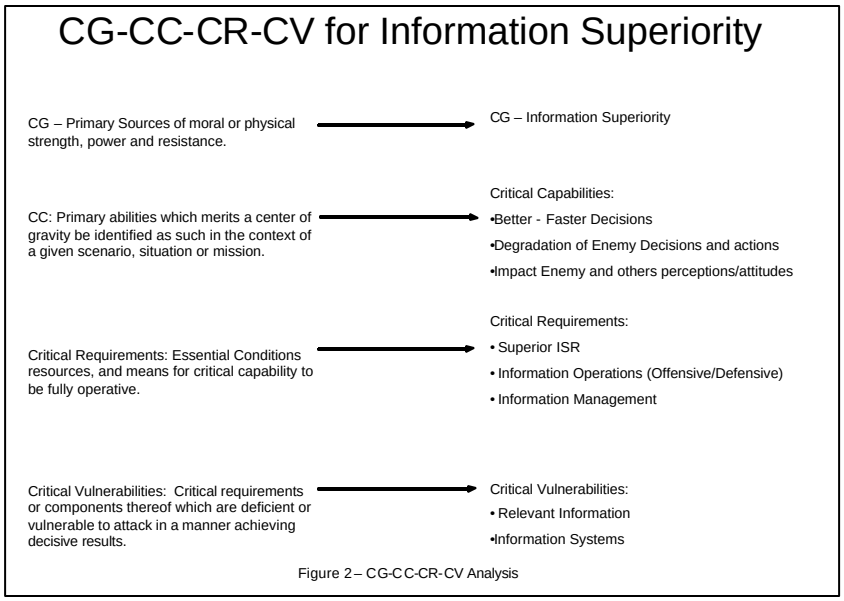


Figure 2 – CG-CC-CR-CV Analysis

[15] Strange, 3. Dr. Strange argues that this a return to the Clausewitzian model, however it could be countered that Clausewitz argues for one center of gravity whereas by his definition Dr. Strange implies there may be more than one. .

[16] It is understood that the center of gravity for a military operation would be something other than information superiority. The use of IS as a center of gravity was designed to show a logical path to its vulnerabilities. Within the context of an operation a center of gravity may have a critical capability of IS which would lead to the same endstate. However, for simplicity sake IS will be examined as the center of gravity.

The attaining of information superiority provides the primary source for gaining the operational advantages. The critical capabilities then become the operational advantage of better decision-making. They are the abilities we wish to exploit or in Dr. Strange's terms, they merit the identification of information superiority as a center of gravity. The critical requirements then become the three interdependent legs of information superiority; ISR, information management, and IO. They are the means and resources that must be effective for the success of our capabilities. The critical vulnerabilities that fall out of this analysis are then information systems and relevant information. They become vulnerabilities because of their componency to information superiority. All three legs within information superiority are supported by (INFOSYS) or strive to provide (relevant information) one of these two items. (Referring back to Figure 1, **Letter A** = relevant information/ **Letter B** = INFOSYS) This analysis seems to make logical sense until you examine what exactly relevant information and information systems are. They are the key components of information management. If we accept that the key components of information management[17] are vulnerabilities, then by further examining doctrine we can develop a means to protect them. This is what the model attempts to provide to the user; the identification of an exploitable vulnerability that requires protecting. This would be the logical flow. However, before asserting this claim a doctrinal look at information management must be conducted.

Understanding Doctrinal Information Management

The first step in assessing doctrine is to evaluate the definition of information management. Information management, according to FM 3.0, is "the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision-making." It has two supporting components. The first are the

[17] As mentioned earlier in chapter one, IO and ISR both have critical vulnerabilities but they are

information systems (INFOSYS). INFOSYS are the equipment and facilities that collect, process, store, display, and disseminate information. These include computers (hardware and software) and communications, as well as policies and procedures for their use. The second component is relevant information. Relevant information is all information of importance to commanders and staff in the exercise of command and control.[18] These definitions are sufficiently vague to constitute good Army Doctrine. However, information craves specificity and this may be where the doctrine lacks.

Chapter 3, FM 6.0 attempts to provide more granularity regarding information management. It labels information management as the science part of control. Information management is said to "narrow the gap" between missing and present information. It suggests the commander provide guidance on information management thereby increasing his decision-making capabilities. FM 6.0[19] suggests using the following factors as guides:

- Degree of willingness to cope with uncertainty
- Information requirements for decisions
- Ability to describe his intent and situational understanding.

Having stated up front that information management is about the science of control, it seems odd that the remainder of the discussion is regarding the art of command. The attempt to place the burden of information management on the commander is made, but the linkage between science and art is blurred. This is clearer in the next section of the doctrine.

Following the "artsy" discussion, the activities of information management are highlighted; collecting, processing, storing, displaying, and disseminating. Once again, the doctrine starts with a clear picture, collection processes (push or pull) but then jumps to

---

beyond the scope of this paper.

[18] *FM 3.0*, 11-11.

[19] *FM 6.0*, 3-11.

dissemination. Only after a paragraph or two discussing the last function (dissemination) does doctrine return to the processing of information. This disorganization causes confusion in understanding the overall intent of the activities.

The manual attempts to clarify the information process by using a cognitive hierarchy. Figure 3 demonstrates the processing of information in a doctrinal format.

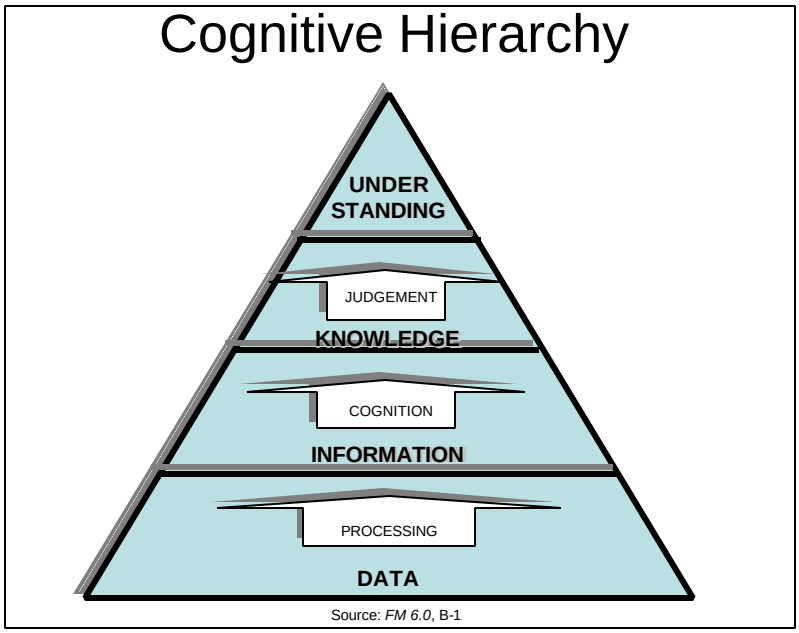


Figure 3 – Cognitive Hierarchy

The diagram attempts to portray a linear progression of information value enhancement that ultimately becomes understanding at the command level. The specifics of the process exist in Appendix B – Information of FM 6.0. Essentially the hierarchy outlines definitions of information progression. Each defined terms raises the level of the data. Data is at the bottom of the hierarchy and defined as the raw signals from the environment not processed in any way. From this step it moves through processing or the assignment of meaning, to become information.

Doctrine states that "it is important to understand that information alone has no meaning"[20] and that further analysis and evaluation provides the meaning in the form of knowledge. Finally, by applying judgment to the synthesized knowledge, information reaches the final level of the hierarchy – understanding.

When reading this process in the manual one aspect remains unclear. The true purpose for the cognitive hierarchy is never established. The analysis conducted results in the assumption that the heirarchy's true purpose is to provide a framework of information; one of the criterion used in assessing Army information management doctrine. The hierarchy is an admirable attempt at providing a framework. However, the problem lies in the fact that it is too "hierarchical" and discounts the ebb and flow of information and more importantly people. The triangular process makes it seem as though you must travel through each step to get to the top. Reality is of course much different. In Richard Wurman's Information Anxiety2, he states "understanding should be continuum from data to wisdom.[21] The distinctions between the steps are terribly discrete but they do exist on some levels…This is mostly due to the fact that at (the understanding) end of the spectrum, it gets increasingly personal until it is so intimate that it cannot truly be shared with others."[22] If Wurman is correct in his assertion, the shades of gray eventually blur beyond recognition then a cognitive hierarchical model is too rigid. This analysis may be considered too critical and ultimately splitting hairs. This would be true if the model set the stage for a further discussion on information management principles. However, it does not. Doctrine discusses a conceptual framework and immediately takes a leap into the prescription of information products without ever identifying any information management principles.

---

[20] *FM 6.0*, B-1

[21] Information Anxiety2 uses Wisdom not Understanding as the ultimate goal of the process. Additionally, the process is one of Understanding – not cognition which is simpler to understand and explain.

[22] Richard S. Wurman, *Information Anxiety2, (*Indianapolis, IN;QUE, 2001), 27

The remaining pages within the appendix discuss METT-TC and relevant information. It is assumed that a discussion of METT-TC is not required and a focus on relevant information is more useful. The bottom line for relevant information is that it has two purposes; develop a common operational picture and develop executable information. If data, knowledge, wisdom, or information does not fit those two categories, it is irrelevant information. The prescription provided to develop relevant information is the Commander's Critical Information Requirements (CCIR).[23] Through these, the commander receives the understanding required to make decisions. It is a simple enough process. Additionally, the doctrine states "IM should focus on CCIR first". This statement presumably intends to provide further guidance on gathering relevant information.[24] Once again, it fails.

This is the point where the confusion reigns supreme. Doctrine instructs one to focus information management, which consists of relevant information and information systems, on the CCIR. This statement is simply unclear and useless. Ultimately, the statement establishes that the U.S. Army Doctrine does not have a real grasp on what information management is or what it does. A quick review of the contradictions is helpful in highlighting this problem.

The information management definition describes products not process by stating it is the "provision(s) of relevant information". This is furthered by the prescribed guidance suggested for commanders that all specify products not process. The statement to "focus information management on CCIR first" solidifies this product focus.

The attempt to demonstrate a framework through the cognitive hierarchy fails because it is too rigid in its design and too loose in its definitions. This could have been rectified by a

[23] CCIR includes Priority Intelligence Requirements (PIR) and Friendly Forces Information Requirements, Essential Elements of Friendly Information (EEFI), and Information Requirements (IR).

[24] *FM 6.0,* B13-16.

discussion on principles of information management but this is noticeably absent from the doctrine.

Finally, and the most frustrating is the organization of information management concepts within the doctrine. The reader must synthesize three chapters and one appendix to gain even the foggiest appreciation of what is being written. This type of organization works if you are product focused but to demonstrate a system it fails miserably. This is probably the most telling of all the contradictions and misstatements.

The challenge is simple. Information superiority is vulnerable in the least defined aspect of its parts – information management. The CG-CC-CR-CV analysis in figure 2 clearly shows that relevant information and INFOSYS are critical vulnerabilities. If they are, by definition, parts of information management then the need to address this concept clearly in doctrine is essential to obtaining information superiority or more importantly operational advantages.

The need to move away from a product focus found in doctrine is clearly established. The way to move towards this goal is to look at several key aspects of the doctrine and suggest alternatives. The first is the definition of information management. The current definition leads down the path of product development. Without a new definition, the rest of the problems moot. The next step is to suggest a framework for information management. The framework must be a conceptual model that can apply throughout all levels of the Army. The framework must support and strengthen the hierarchy found in Figure 3. Finally, there is a need for principles for information management. These principles will add substance to the doctrinal terms and provide guidance for the planning and execution of information management. By addressing these aspects, doctrine can then provide a clear and coherent picture of what information management is and can provide to the Army. The establishment of a sound doctrinal base then supports information superiority by addressing one of the key vulnerabilities.

CHAPTER THREE

Information Management – A System View

Redefining Information

The previous discussion centered on providing an analysis of information management current doctrine. The approved Army definitions and terms for information superiority and management were evaluated. This analysis demonstrated the Army's focuses on information products not a process. By stating that the two parts of the information management are hardware (INFOSYS) and relevant information, misunderstandings and mismanagement can occur. To take a systems approach for information management is clearly the answer. This chapter provides the essential elements to assist in developing a systems approach for information management. By using three of the four criteria[25] identified earlier (the definition of information management, a framework for the process, and principles for implementation of information management) along with business models and academic writings, concepts and principles are put forth for consideration. Current doctrinal strengths coupled with these models result in practical solutions for Army information management.

The initial step in this process is to define correctly the term information management. The last chapter demonstrated that the Army uses a product focus definition that results in a complicated and ineffective information doctrine. The best way to correct this problem is to breakdown the term and clarify each part.

[25] The last criterion, organization of information management doctrine is addressed again in the conclusions and recommendations chapter.

There are three schools of thought on defining the term "information"[26]. The first is describing information as a message. This is the classic view. It has been used and cited most frequently. Most dictionary definitions take this approach. The focus for this interpretation is on reports, orders, and instructions. A result of using this definition is a hierarchy view of information as seen in Figure 3 (Cognitive Hierarchy). The Army subscribes to this view. The Army states that information is the meaning associated to data. This "meaning derived from data" is clearly a message that is intended to control actions. This is a simple way to describe information and on the surface an easy to understand definition. The problem with the definition is that it does not provide tangibility to the subject. One of the most difficult thoughts to develop is a tangible definition of something that is inherently elusive. Nevertheless, tangibility is critical to add clarification to a term or subject. Without a common, concrete, and clear definition, information is subject to individual interpretation. This causes confusion and works against the entire process.

The next view of information begins with the "message" definition and expands it to include the transmission medium. This definition describes information in the terms of the process of transmitting and receiving the desired signals. This view of information takes into account the complexity of the information networks and attempts to better define the concept of information as a process. The failure of this definition is that it still relies on an intangible view of information that is difficult to conceptualize. It also focuses more on the transport of data than on the use of it. Simply put, this is the classic encoding and decoding information model. These two definitions are simple and straightforward attempts to recognize what information is and what it must do. However, they do not assist an organization that recognizes the need to dominate the "information environment". Because the Army has a stated objective to accomplish

[26] John Arquilla and David Ronfeldt, *In Athena's Camp.Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997) 145. The following paragraphs outline the three views of information as described by this document.

this dominance, these definitions are of no real use. In recognition of this, the next definition of information has been developed. It is more contemporary and addresses the weaknesses of the previous two.

The view of information as a physical entity is another definition commonly used. The genesis of this view is the need to create a tangible definition that incorporates information into an organizational structure. Blaise Cronin and Elisabeth Davenport suggest a relatively simple view that meets this need. They define information as an asset.

Cronin and Davenport use this term as a way to convey the importance of information to business managers. The use of the word asset raises the awareness of information as a valuable commodity within an organization. By describing it as a physical part of the organization, it can then be manipulated, stored, distributed, and valued in the same way as other assets (i.e. capital and employees). Once it understood to be an asset, categorization takes place enhancing its utilization. Most research on information overload, points to categorization as the key component to avoiding misuse and paralysis. In its simplest form, categorization refers designing storage containers (by type) into which information is placed, classifying or categorizing incoming information into those containers, and providing a method to deliver information to end users[27]. The essential element of categorization is to define what categories are required. Blaise and Cronin offer a solution.

At a minimum, information is placed into three sub-categories; public, merit, and private. The public information generates a community good. Although not specifically tailored to the business it is provided for general use. Merit information provides benefits for the collector and

[27] Multiple reference sources stressed the need to categorize information to ensure its timely use. However, most of them address specific "product" focus solutions or technical solutions. For more information regarding these techniques see: James R. Dukart, "Content categorization: Making sense of information overload," *E-DOC*, (January-February 2002), 24.; Maryann Lawlor, "Information plus context equals knowledge" *Signal* (February 2002), 37-40; Reid Goldsborough, "Breaking the information logjam," *Consumer Research Magazine* (June 2002), 30; Keith D. Denton "Better decisions with less

other joint users. Finally, private information is only beneficial to the collector of the information.[28] These categories are relatively simple. They do not provide for all the needs of an organization but they do illustrate a way to view information as an asset. More importantly, the categories begin a process of adding value to information. This is the main objective of using the term asset for defining information. If a common understanding of assets exists, then an appropriate value can be assigned and ideally lessen the waste associated with information. Waste, defined as either the lack of energy or excessive energy directed towards an information category, is another factor in information overload. Avoiding waste obviously reduces opportunity for overload. Cronin and Davenport state simply that value only exists if the information is appropriate to a task at hand.[29] In other words, if the information does not have a need, measured against a category, then it is not required and thus wasteful.

To understand value measurement of information specific types of "values in use" are identified. Table 1 provides value types as identified by Cronin and Davenport.

Table 1 – Types of Information Value

Value in Use	Application/Transformation/Comparison
Exchange Value	Price or Equivalent (what are you willing to pay for the information?)
Option Value	Decision to Use of Not to use
Insurable Value	Replacement Cost (Rebuild database/Archive)
Latent Value	Unappreciated Value (realized when circumstances changed)
Covert Value	Valuable because it is hidden
Integrative Value	Completeness of Knowledge

Source: Blaise Cronin and Elisabeth Davenport, *Elements of Information Management*, (Metuchen, NJ: The Scarecrow Press, 1991) 73.

information," *Industrial Management* (July-August 2001), 21-25; and Kenneth Preiss, "A two stage process for eliciting and prioritizing critical knowledge," *Journal of Knowledge Management* (2000), 328-336.

[28] Blaise Cronin and Elisabeth Davenport, *Elements of Information Management*, (Metuchen, NJ: The Scarecrow Press, 1991) 34.

[29] Cronin and Davenport, 69.

The establishing of a "value in use" adds to the worth of the asset. It provides a clear description of why the information is required and furthermore, how it may be used. In a military application, this type of value analysis allows the commander to direct the energy of his staff. The staff is clear on the importance (value) of the information desired. For example, if the value of certain information were described as having a latent value it would be categorized as being public and stored for use when the situation dictates. Additionally, the task to obtain the information would not receive the energy or time that an "option" use information type would have. Conversely, an "option" value information requirement categorized for merit use receives the appropriate resources and dissemination.

This type of thought process promotes the understanding of information as a valuable asset measured and used in appropriate forms. This is not a checklist but rather a way of viewing information similar to the classes of supply. For example, each supply category receives a priority (measured in worth) by phases and emphasis added or removed in concert with the operational needs. Information receiving the same value measurement allows the system to function more efficiently. Arguably, on certain levels this type of process takes place. Commanders direct the staff to gather information critical to certain aspects of an operation. The use of CCIR and PIR provides for a type of value measurement. Conversely, the counter-argument is that within doctrine there is no discussion of value measuring or asset usage. The doctrinal definition does not address the need for tangible and a common understanding of information values. The vagueness of the term "relevant information" does not provide a measure of value. A more clear and usable measure of value is needed to insure the proper, timely, and accurate information is sought out and delivered. Information defined as an asset provides this type of framework for measurement and usage. Finally, the understanding of an asset allows for its placement into a system as well as its careful expenditure. However, defining

information is only part of the equation. The next step is to define the term management as it relates to this overall process.

Redefining Management

Management is a system comprised of functions. It is commonly agreed that there are five functions of management; planning, organizing, staffing, directing, and controlling. A simpler way to define management is refer to it as the act of problem solving.[30] With the acceptance of this as the basis for management, it is clear that a limited "product" view of information management lacks the depth to be effective.

Each of these functions has an important role in the management of information. A brief overview of each will assist in establishing this crucial linkage. The first function is planning. Planning involves the establishment of objectives and procedures or policies to accomplish the goals. Dale E. Zand states that the key to effective management of information is to ask the hard questions up front. These include;

1. What information is worthwhile?
2. Who has the information? Or should have it?
3. Who should receive the information? Why? What is the expectation once it received?
4. How can we improve the way we collect and disseminate existing and future information?[31]

---

[30] Bernard L. Erven "Creative Problem Solving" *The Five Functions of Management.* n.d. <http://www.ag.ohio-state.edu/~mgtexcel/function.html> (10 November 2002).

[31] Dale E. Zand, *Information, Organization, and Power – Effective Management in the Knowledge Society.* (New York: McGraw-Hill Book Company, 1981) 9. Additionally information on this approach is found in, John Hodge, "Enlightened Knowledge Management," *Insurance and Technology*, (June 1999), 59-60. His article provides additional insights and pitfalls to avoid when planning for information technology.

The goal of the planning for information is to reduce uncertainty within decision-making. It establishes what is required to make a decision and places information in the categories described earlier. By assigning information a measure of value, it becomes usable. Failure to accomplish this results in irrelevant or unusable information. Finally, through the planning function the question of what information is unobtainable needs asking. This question prevents wasting valuable assets. Ultimately, answering these simple questions establishes a path for information as it moves through the management functions. If the manager does not ask these questions, the remaining functions do not accomplish the desired outcome - a maximum utilization of the information.

Organizing and staffing functions are closely related. Organizing is the function of setting up the structure within the organization to achieve the goals laid out in the planning function. Staffing involves placing the proper people in the structure established to ensure success. This involves resourcing the staff with the proper tools to accomplish their mission. Resources include training as well as equipment. The next section addresses organizing in-depth using a business model. A key to both of these functions is the empowerment of the individuals to accomplish their jobs. The establishment of the organization must be well-defined providing clear lines of responsibilities to avoid duplication and the more dangerous seams.

Directing an organization best described as the leadership function within the military. It is different from the controlling function in this regard. The leadership role focuses on the motivation or influencing of the individuals through personality and example. Controlling involves the measuring, reporting, and correcting of overall objectives within the organization. Simply put, the directing would be more of an art versus the science of control.

Using these accepted functions of management as the foundation for defining management, it is apparent that the combination of both assets (information) and a process (management) are the keys to success within information management. The limited view of

information management defined as relevant information and INFOSYS clearly does not meet this need.

Arguments exist that the Army addresses some of these functions in military decision-making process (MDMP). For example, the mission analysis identifies tasks, facts, assumptions, limitations, and constraints, all of which are part of the management functions. The counter-is that the MDMP does not specifically address the development of the information management plan as it does the overall operations plan. It identifies information requirements but does not clearly stipulate all the required functions and controls within the process required for proper information management. Finally, if as doctrine states, information superiority is required on the modern battlefield then more clarity and analysis to protect its vulnerabilities must be conducted.

This discussion of management functions has established the need to re-look the definition of information management. It provided an analysis of business applications measured against the Army information management definitions. The definition of management as a five-function process provides a broad outline for revising the Army's view of information management. Finally, it demonstrates that the vaguely addressed planning function in the MDMP requires more emphasis. Achieving this emphasis requires an examination of the "organize" function within information management. The next section provides this examination. It establishes a model that organizes information management into an understandable and effective framework.

Information Management – A constitutional framework

The establishment of an organization that exploits the information it gathers is the simply stated goal of the Army in Vision 2010. The monograph addressed this in the first few pages. Doctrinal weaknesses suggested a suggested redefinition and comprehension of the process of information management. This process began in the last section with redefining information

management. The next step is to discuss the organization that is attempting to gain information superiority. This is the essence of the second criterion for evaluating Army information management doctrine. An established and understood framework for information management provides the necessary foundation to gain and maintain information superiority. As demonstrated in the previous chapter, the current doctrine does not provide for this type of framework. This next section addresses this issue.

If knowledge is power then the control of knowledge leads to greater power. This is where many of the problems of information management lay. The organization itself prevents proper management of information for a couple reasons. One is the structure of the information environment and the second is lack of policies and procedures. Because the nature of information environment is such that the commander cannot control it all, he must then dominate that which he does control. This is the position that Paul Strassman argues in his book *The Politics of Information Management* and it has great applicability in the Army.

The wrong version of software, the wrong variable for the security device, no available "drops" for new computers, and the STU-III key is invalid. These are normal everyday occurrences on an exercise or deployment for a communications staff. How are these simple items overlooked? Strassman would argue that it occurs because managers do not understand the policies or the environment in which they operate. . The lack of buy in for policies at the operator or business level causes individuals to do what they believe is best. In other words, the users either (1) do not know the policies or (2) choose to ignore them. This results in a snowball effect for the entire organization. He states "companies that dedicate their information resources principally to internal coordination instead of deployment for the benefit of external customers do not realize the benefits – regardless of the technical excellence of their application."[32] Although

[32] Paul A. Strassman, *The Politics of Information Management – Policy Guidelines*, (New Canaan, CT:The Information Economics Press, 1995) ,23.

that statement is focusing on business and its customers, the application to military forces is readily apparent.

If sections within an organization, for example the Intelligence Section (G-2), develop a system that works independently of the existing structure the usefulness of the system is suspect. The technical problems can overwhelm the network to a point of failure. If this type of "stovepiping" is the norm within an organization then its overall effectiveness downgrades exponentially. Instead of achieving information superiority, the organization achieves paralysis. For example, a section independently shifting assets to support a private, latent value, information requirement at the expense of a more pressing merit, "option" system begins to derail the overall process. The slippery slope is apparent in this example. So what is the fix?

Strassman advocates a federalist concept of information management as the solution to this problem. This view suggests "the politics of information management concerns the balancing of interests between centralized control and decentralized execution."[33] Simply put, it models the U.S. Constitution concept of individual freedoms balanced by a common law resulting in an overall balance and effectiveness of information management. This concept embraces the rights of individuals to achieve the desired information superiority through means that follow the guidelines that are acceptable within the framework of the "constitution".

This concept sounds inherently bureaucratic; though it is not in practice. The argument centers on the need to have a stable plan for information management. Strassman argues that the greatest obstacle in the management of information is the volatility in governance. Constant changes in procedures, personnel, and policies result in a lack of common understanding. The suggested solution is the establishment of agreed upon and enforced policies. His belief is that information management is a deliberate plan, encompassing information handling, knowledge preservation, communications, and learning functions. Finally, he states that confusing the

[33] Strassman, XXIX.

management of information with supporting technology is the primary reason why comprehensive information designs fail in integrating the overall organization plans.[34] As stated earlier in this monograph, technology is a tool to support information management. Failure to recognize this crucial point results in a technological solution that is short-lived and ultimately flawed management of information.

The success of this constitutional model relies on the commander. This is fitting for several reasons. First, as with all critical assets within an organization the commander should be intimately involved in its use. Second, to enforce a program or policy requires influence and control. This is clearly a command responsibility. Third, the entire aim of information management is decision making by the commander. With this as the stated aim, it is clear who should direct the overall framework. Lastly, this concept is not too far off from the current doctrine in which the commander has the responsibility for providing guidance and direction. However, the difference in this model is that he is not providing specific requirements but rather a framework of thought. This does not remove the current CCIR or PIR, rather suggests a framework for governing the gathering and processing of these requirements.

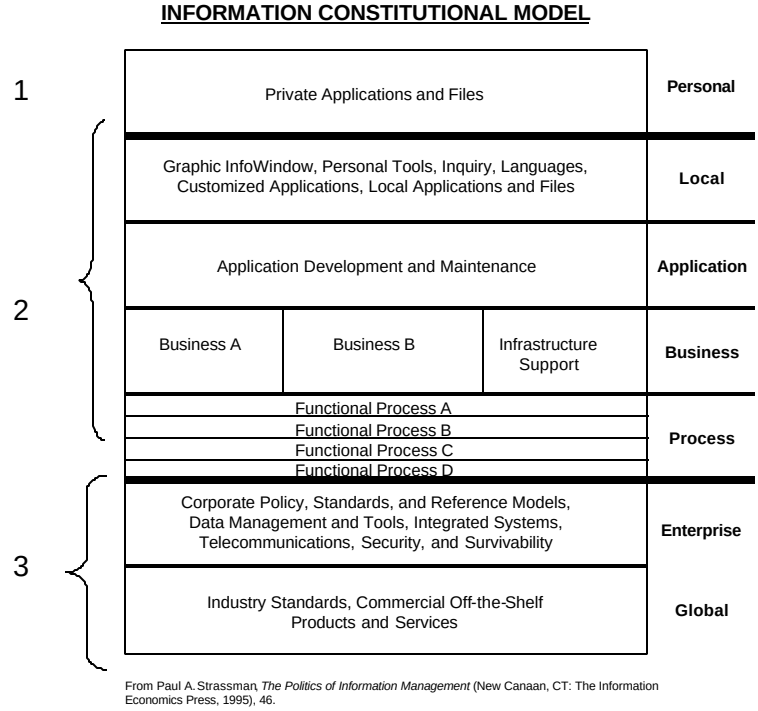
The command responsibility does not remove the staff from the constitutional framework. Strassman suggests that because individuals cannot make their own rules and still expect order, there must be a central control. In the Army, that would be the commander. However, the staff and subordinates must still be involved. He argues this by stating "to manage information successfully, policy makers must set forth explicit principles for information governance and secure cooperation by engaging everyone in a discussion as to their implications. Full disclosure of the rules for governing must indicate who will deliver what results and how policy will be enforced."[35] The key to the engagement process is to have the correct people work the policies. This should not be the technical experts but rather decision makers and key

[34] Strassman, 17.

personnel in support. One of the greatest dangers in information management planning is delegating the responsibility to a technical expert.[36] No matter how talented, this individual has a different focus than a manager and this view skews the process.

The constitutional model Strassman advocates is one that has direct command involvement, clear guidelines, not technical focused, involves all key personnel, and protects individual information requirements rights. The question then is how to apply this in practice.

Strassman provides a model and it is depicted here as Figure 4. This figure represents, according to the author, the most complicated view of the constitutional model. Within the Army, the model would have similar aspects but modified to meet the specific needs of a military organization. The key concepts though are applicable as will be shown in the next few pages.



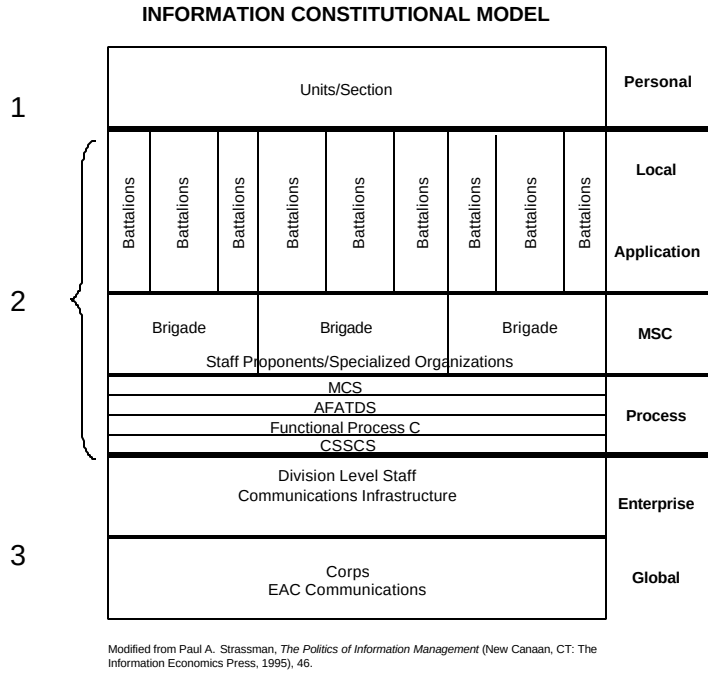
From Paul A.Strassman, *The Politics of Information Management* (New Canaan, CT: The Information Economics Press, 1995), 46.

Figure 4 – Constitutional Model

[35] Strassman, 5.
[36] Strassman, 5.

This model revolves around seven layers broken into three major groups. The labels on the left (1-3) refer to the major groups. The key to understanding this design is not to draw a direct "line for line" correlation between the military and this model. For example, Group 3 does not exactly equal the Department of the Defense and Department of the Army or Group 2 is not the Corps through Battalion Level.

Although the design of the constitutional model is hierarchal in depiction, the system is not a top-down or bottom-up process. Earlier in this paper, we attacked the Army's linear model. Is this model not similar? The answer is no. The difference within this design is the provision of a mental picture for comprehension. The model has a remarkable resemblance to what a constitution would look like. Thus provides a tangible framework to follow. The Army model used definitions to demonstrate the flow of information. The descriptions lent themselves to a linear and hierarchal thought process. The Strassman model does not; it is a conceptual mental model. With this difference in mind, what does an Army Framework resemble?



Modified from Paul A. Strassman, *The Politics of Information Management* (New Canaan, CT: The Information Economics Press, 1995), 46.

Figure 5 – An Army Example

In drawing a constitutional framework for the Army, it could look like Figure 5[37]. Remember the caveat; the model only demonstrates a constitutional picture. The intent is to provide a mental picture illustrating the hierarchy underlying an information management system. The hierarchy does not present the system of managing information but rather the framework for establishing the plan for management of information. It is for that reason that the model is successful in presenting its argument.

The picture establishes a process for managing information within a framework that promotes understanding at all levels of an organization. Simply put, all parts of the organization understand where they fit into the process. The model presents three key parts; standards and policies (Group 3), functions and applications (Group 2), and the user responsibility (Group 1). In a military setting this is best described as the commander, the staff (or functions), and the soldier behind a keyboard. All of these parts comprise the system that produces the desired results – information management.

Another key aspect of this argument is that the system must encompass all aspects of the organization including its external requirements. A design that focuses on internal applications and functions isolates itself from the other key elements to the model. For example, selecting a software suite that does not support the policies and standards or incompatible with the equipment a user has results in a breakdown of the system. The model establishes a clear understanding of the need to integrate all aspects of the organization to ensure a properly functioning system.

When examining this framework, an argument exists that the Army has this in place by the normal chain of command or task organization. The counter to this argument is that

[37] This model follows the Strassman method of showing the most complicated and robust picture. In reality, the constitution established would reflect the unit/organizations needs at the levels desired. The key would be establishing the three main groups – standards and policies, applications and functions, and user.

information management, although a command responsibility, is not by default equal to task organization. A conscious effort to understand where each policy, application, and individual fits into the overall information architecture is required to ensure proper management. The framework in Figure 5, although seemingly complicated, is in fact the easiest solution to information management. It is Corps managing information in an environment that it can control through a normal chain of command. Unfortunately the current operating environment involves units be sent to perform missions outside the normal context of Corps-Division-Brigade relationships. This type of situation requires a detailed plan for outlining the policies, applications, and user level responsibilities. Failure to outline these simple, yet intricate relationships will result in a product versus system management of information. The constitutional model does not to provide a strict adherence to a task organization but rather a flexible framework that allows the system of information management to function. Keeping the three key aspects of the model (policies and standards, applications and functions, and users) as the baseline for planning ensures success in achieving this goal.

Principles of Information Management

Strassman's constitutional model demonstrates that a significant amount of planning is required to establish a coherent and usable model. This planning results in an organizational design that sets the conditions for a system of information management. When developing a plan it is useful to use a guideline or set of principles. The Army recognizes this truism and provides several tools to use. One is the elements of operational design and another is the principles of war. The first provides a framework for the plan and the second provides simple rules to use in evaluating and filling in the framework. As demonstrated in this monograph, a similar framework for information management did not exist in doctrine. Strassman's constitutional framework fills this void but the need to address the third criterion still exists.

An essential criterion in measuring Army information management was the evaluation of principles for information management. The evaluation process was quite simple; none existed. However, before delving into the concepts principles of information management, establishing a context is crucial. FM 3.0 states that the principles of war are "the enduring bedrock of Army doctrine but they are not a checklist. They do not apply in the same way to every situation. Rather, they summarize the characteristics of successful Army operations. Their greatest value lies in the education of the military professional. The principles of war are powerful tools for analysis."[38] This understanding of principles is the context for presenting the following principles of information management. They are not all inclusive or exclusive. The intent is to provide a way to evaluate the way in which an information management framework is established and used.

There are 13 principles of information management identified by Morton Meltzer in his book *Information; the ultimate management resource*[39]. They are listed below in Figure 6.

---

[38] *FM 3.0*, 4-12.

[39] Meltzer, 153. All the principles are discussed individually. Rather than citing each paragraph independently, the chart is cited with the intent of being inclusive for all the principles.

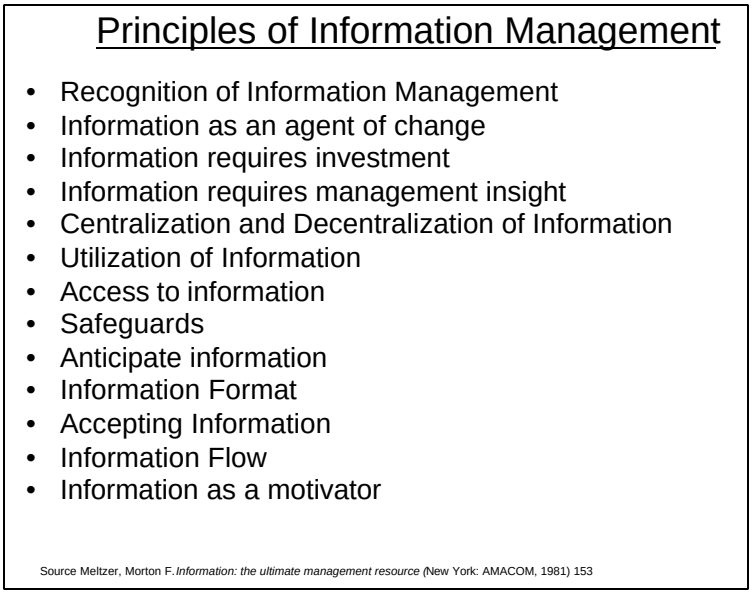


Figure 6 – Principles of Information Management

The first principle is the recognition of the need to manage information. It is simple and direct. The success of an information-based organization directly relates to the identification of this need. It is the first principle because the failure to recognize this need invalidates the remaining principles. Arguments exist that this is not a required principle. The counter is that this principle stresses the need for a systems approach to information management. For this reason, it is a central thought that must thread itself through the entire framework or design.

Although the principles are not listed in an order of priority and all should be weighted equally, some principles are more equal than others are. The principle of information as an agent of change is one of these cases. The discussion of this principle occurred earlier in this paper in the description of the changing battlefield due to increased information access. Essentially, this principle is the solidification of the concept that information facilitates the desired goal of obtaining operational advantages. It highlights the impact that information has on the organization – both positive and negative. By understanding this goal of information superiority at the beginning of the design process, the remaining principles become clearer.

The next principle is that information management requires investment. Often this is mistaken for just a capital investment in technology. The investment actually refers to three components. The first of which is the capital investment. This is important but not so as important as the investment in the second two; personnel and time. The investment in personnel involves training and developing them into information workers. The immediate thought that comes to mind when stating that training and developing of soldiers is that it must be technical. This is not necessarily the case. GEN Bell addresses this issue in his article for *ARMOR* magazine. He states that the need for developing soldiers for the information environment is more important than just training them on technology. An investment in creating adaptive, agile, and decisive leaders is the key to success.[40] This thought process is clearly the correct approach towards creating a system of information management and leads directly to the next principle.

The need for insightful managers is critical to information management.[41] Earlier in the paper, we established the command responsibility for information management. Leaders with the understanding of the system and directly involved in the process ensures that the framework established meets their organizations information needs. It also ensures the support of the investments required for information management. Insightful leaders also enforce the principle of centralized policies and decentralized information. The centralization of policies and standards (Group 3 in Strassman's model) assists in the ease of decentralized information sub-systems functioning together.

The next principle intends to solidify the definition of information described earlier in the paper. The principle of information utilization essentially states that the creation of information

---

[40] Bell, 42.

[41] More information on insightful managers can be found in; Bill Ringle, "What every business manager should know about knowledge management," *The Canadian Manager* (Summer 2001), 11-27. The author outlines five key points that assist managers. They are; the need to know what is knowledge from what is data, the need to champion the cause, and the need to see where to start, the need to jumpstart the process, and the ability to track results.

does not ensure its use. There must be a requirement for information or it is a wasted asset. If the information management process produces information that has no rhyme or reason then the process is flawed.

One way to assist in producing information that has utilization is to incorporate the principle of access of information[42]. This principle states that information access should be encouraged and facilitated. This should be proportional to the principle of safeguarding information. This principle usually refers to the protection of sensitive information. Nevertheless, it is not just the protection of military networks and classified information but also the protection of individual rights for use of information systems. Although easily overlooked, the need to create an environment for open and frank information sharing involves protecting individual's private information. Polices and standards must address this issue before the problems arise.

The next principle is that a good information management plan anticipates information requirements. It is a goal to provide information not just from requests but also from anticipation. This allows the decision maker to take action and not be reactive. This principle manifests itself in the questions that Zand ask during the planning process. Essentially, the system should ask how many conditions have to change for a decision point or what new conditions cause a new decision.[43] By addressing these questions in the design process, the information management process anticipates critical questions.

It is important to provide information but the next principle addresses what it should look like. The principle of information format revolves around two key tenets. The first is that the information should be in format that is usable by all the required parties. This follows directly

[42] Two articles that provide more information on the need to share information are; Julian Birkinshaw, "Making sense of knowledge management," *Ivey Business Journal* (April 2001), 32-36 and Nancy Dixon, "The neglected receiver of knowledge sharing," *Ivey Business Journal* (March-April 2002), 35-40.

[43] Zand, 10.

into the second tenet that information format should not be determined by the technical staff but rather by the users. This is a simple rule but often the reality is the other way around. If the intent is to provide information to decision-makers then the format is their decision. This relates directly to the standards and policy functions of commanders. Formats should be clearly stated, understood, and most importantly enforced. A lack of policy enforcement leads to loose controls and ultimately a breakdown in the system. The information format is important as stated above but it should not be so draconian that it impedes system. Simply stated, if pen and ink changes are acceptable – then they are acceptable

The next principle is accepting information. This principle is not just about being open minded and accepting information provided but also includes accepting the process required to develop an information management system. Embracing the investments required and adding to the collective knowledge developed. This concept affects the next principle, information flow.

In the contemporary operating environment, innumerable sources transmit and receive information. The flow of information is a critical part of the framework within information management. The challenges are to breakdown the existing vertical barriers and produce a truly networked system. Success equals a system accessible, shared, and improved by all the members of the organization. This also involves the inclusion of external sources. Successful information flow is a continuous process. One of the benefits of creating a continuous and networked information flow is that it supports the last principle of information management.

The principle of information as a motivator is the result of embracing the previous principles. The inclusion of all members in an organization in the information loop empowers them to do their jobs. Information allows all members of an organization to understand its overarching goals, which leads to a common vision. The elimination of stovepipes and information vacuums increases the overall knowledge of the organization. This allows an organization to work in a common direction with an understood purpose. This results in the

improved performance of the organization. All of these factors continue a circular process of motivating and increasing performance of the organization.

The intent of the last few pages was to establish the baseline definitions of some principles for information management. If taken individually, their impact on the development of an information management system is negligible. The power of their use then comes from the understanding of them as a group of concepts identified to help develop an information management framework.

The discussion within this last section has provided a baseline for development of a framework and principles for use in information management. The mission was to analyze three specific areas of information management: definitions, frameworks, and principles. The intent was to provide concepts on each for further development within Army doctrine. Using these concepts as a model, the next chapter of this monograph provides conclusion and specific recommendation for their use in Army doctrine.

CHAPTER FOUR

Conclusions and Recommendations

Army leadership identified information superiority as one of the key elements of success on the current and future battlefields. The second chapter of this paper addressed this concept and demonstrated that information superiority was vulnerable in the least defined aspect of its parts – information management. The CG-CC-CR-CV analysis in Figure 2 demonstrated that relevant information and INFOSYS are the critical vulnerabilities. If they are, by definition, parts of information management then the need to address this concept clearly in doctrine is essential to obtaining information superiority or more importantly operational advantages. Additionally, the most frustrating aspect doctrinal information management of is the organization of the concepts. As outlined earlier in this paper, there is no central reference addressing information management in its totality. Doctrine spreads the concept throughout multiple chapters and appendices. This disjointed organization furthers the problem of a product versus system view of information management. This was the starting point for this paper. Doctrine describes information management as product oriented but to achieve the stated goal of information superiority, it must be a system.

The approach taken to solve this problem was to evaluate current doctrine against four criteria. These criteria addressed definitions, frameworks, principles, and organization as they related to achieving information superiority. Specifically, does the current doctrine on information management support the goal it has set for itself? This chapter will provide conclusion using these criteria and recommend doctrinal modifications for implementation.

As stated earlier in the paper, obtaining operational advantages is the primary reason for gathering, creating, analyzing, and storing information. Any process designed must ultimately support this goal. Specifically, the speed, accuracy, and relevancy of information measured

against the advantages gained by using it. Information management doctrine, in its current state does not support this goal. In, short, we are not prepared to manage the information created on the modern battlefield. With this broad conclusion in mind, the following are specific conclusions.

Conclusions

The first conclusion is that current doctrine does not define information management as a process. It is a product-focused definition. The Army definition of information management states "…it is the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision making"[44]. This definition presents an endstate or product – relevant information. It does not establish the system or process.

Once understood that the current definition does not describe a process, thesecond conclusion is self-evident. Doctrine does not provide a framework for information management. FM 3.0 establishes an Operational Framework and Elements of Operational Design[45] as the conceptual framework for visualizing and designing operations. These models provide the commander and staff with the tools that facilitate the process of planning and execution. Within the area of information management, this type of framework does not exist. The lack of this type of framework denigrates any hope of information management establishing control mechanisms that meet the needs of commanders and staffs. In short, there is no conceptual picture of where each piece of the information environment fits into overall information management.

The third conclusion of this paper is that principles of information management do not exist within current doctrine. Because they do not exist, a critical link in developing a framework for managing information is broken. Doctrine publishes a list of qualities that apply to information: accuracy, timeliness, usability, completeness, precision, and reliability. These are

[44] *FM 3.0*, 11-11
[45] *FM 3.0*, 4-18 and 5-6

not principles of information management but rather traits information should possess. Much like the principles of war, principles of information management would provide a way to think about using the assets available to achieve the goal of operational advantages.

The last conclusion of this paper is in regards to the organization of information management within current doctrine. As this paper has stated information management is a process and not a product. For a process to be clearly understood it must be organized in a consistent manner. Current doctrine fails in this endeavor. The lack of organization impedes the understanding of information management and ultimately prevents its development into processed focused techniques and procedures.

Recommendations

In order to describe information management as a process, the term information requires redefinition. In re-defining information, the Army must look at information as an asset that has worth and measure. This is a departure from the current view of information as a message ("meaning assigned to data"). As outlined earlier in the paper, the current definition used by the Army reflects the past views of information that leads to confusion and too many individual interpretations of terms. The establishment of a tangible definition allows for better understanding of what information is and can be to an organization. It is critical not to view this change as purely semantic. It is a deliberate shift in mindsets. The description and labeling of information as an asset requires, by definition, management processes. It is obvious that the attempt to manage the "meaning assigned to data" is far more difficult than the information asset. This definition is critical to information's relevancy as well as its care and use.

The use and care of information translates into its management. This translation is the second recommendation. The management process must be incorporated in the Army doctrine for information management. The five functions of management (planning, organizing, staffing, directing, and controlling) were outlined earlier in the paper. The incorporation of these time-

tested functions into the information management doctrine provides a means to use the asset of information to achieve operational advantages. Only through positive and a well-defined management process are information assets best utilized.

The redefinition of information and the incorporation of management functions produce a new definition for information management. A recommended definition is the process of planning, organizing, staffing, directing, and controlling the use information for obtaining operational advantages. This definition of information management clearly establishes the overall intent and focus for information management. It does this through two ways. It creates a direct link to the end state of information superiority by establishing the goal of operational advantages. Secondly, this terminology removes the product focus found within the current doctrine and establishes a process focus.

These redefinitions provide the starting point for correcting the deficiencies in current doctrine. Once establishing information management as a process, the next logical step is to provide a framework for its implementation.

The recommendation is to draw on Paul Strassman's constitutional model as the framework for information management. This constitutional model provides the flexibility that allows the process of information management to function within an organized and effective framework. Its use of Strassman's three core ingredients as the baseline assists in the planning for quality management of information. The use of the word assists is intentional. In addition to a framework, a key aspect to planning for information management is to derive principles. These principles then serve as a guideline in developing the Strassman framework. This is the next recommendation of this monograph.

The thirteen principles provide an excellent starting point. When taken together they provide a sound summarization of the key characteristics of a process focused information management. The list, as discussed earlier, is not all-inclusive and certainly can be lengthened or shortened over time. The recommendation is to integrate them into current doctrine and continue

to review and improve upon them. As information management matures within doctrine so should these principles. However, the use of these principles within current doctrine will undoubtedly provide the direction and guidance required to develop an information management process.

The final recommendation provided is re-organize information management within doctrine. Currently doctrine has three chapters and one appendix that pertain to information management. In addition to their disorganization, no one of these sources is comprehensive or clear. This type of organization works if you are product focused but to demonstrate a system it falls short. The specific recommendation is to provide one source that addresses the conclusions and previous recommendations.

The implementation of this recommendation begins with establishing*FM 6.0, Command and Control* as the proponent for information management. The manual should include a stand-alone chapter on information management. This one chapter would then provide the doctrinal definition of information management, Strassman's framework, and the principles of information management. This chapter would set the stage for further doctrine to develop the necessary techniques and procedures.[46]

The discussion of techniques and procedures for information management is the responsibility of FM *5.0*. This manual serves as the central point of reference for Army planning. Therefore, it would be the natural fit codifying information management plans. The recommendation is produce an appendix that outlines a process for establishing an information management plan. Additionally, the manual must demonstrate the need to incorporate information management throughout the Army planning process. Although the scope of this paper did not allow for an in-depth discussion on this subject, it is a great topic for subsequent

[46] This does not suggest a deletion of information management from FM 3.0 Operations. FM 3.0 must address this subject but the details and explanation of concepts should be the responsibility of FM 6.0.

monographs. These two sources, if well organized, will undoubtedly support the overall intent of information management – gaining operational advantages.

This monograph began with the question of are we prepared to manage the information created on the modern battlefield. The answer is currently – No. The information management within current doctrine overlooks the process of managing information and describes immediate, useable products that fit only one decision need. By foregoing the system approach for a single need product, decision-making eventually deteriorates and advantages of information superiority are lost. The intent of this paper was not to provide a better way to process a situation report or "wire a TOC". It was to evaluate the doctrinal defined process of information management and assess if it was usable, complete, and in agreement with the stated goals of information superiority. The recommendations and conclusions addressed in the last few pages are the result of this evaluation and assessment.

The stated conceptual recommendations, incorporated into a in a single source document support the declared objective of Vision 2010 - achieving information superiority. The ability to manage the asset of information required for commander's decisions is critical to the current and future war fighter. The shortfall of current doctrine is that it does not directly support the concept of information management. It focuses on products and not the process involved in managing information. This focus leads to the failure of obtaining the desired operational advantages. The clarification of information management doctrine directly addresses information superiority's critical vulnerabilities. The reevaluation of definitions, establishment of frameworks, and incorporating principles of information management provides the tools to correct this deficiency. By developing a sound doctrinal systems view of information management, achieving the ultimate goal, information superiority, is within reach.

Bibliography

Antal, John F. "Lessons Learned from the fighting in Afghanistan." *Army,* (June 2002): 14-16

.Arquilla, John and Donald Ronfeldt, ed., *In Athena's Camp, Preparing for conflct in the Information Age.* Santa Monica, CA: RAND, 1997.

_____. *Networks and Netwar, the future of Terror, Crime, and Militancy.* Santa Monica, CA: RAND, 2001.

Baldacchino, Kim. "Information Overload: It's time to face the problem." *Management Services,* (April 2002): 18.

Bell, B.B. "Is information superiority all it's cracked up to be?" *Armor,* (March-April 2001): 5,42.

Bruce, Bertram C and Bernard Junwirth, "Information Overload: Threat or Opportunity?" *Journal of Adolescent & Adult Literacy,* (February 2002): 400-06.

Birkinshaw, Julian. "Making sense of knowledge management." *Ivey Business Journal* (March-April 2001): 32-36.

Cronin, Blaise and Elisabeth Davenport. *Elements of Information Management.* Metuchen, NJ: The Scarecrow Press, 1991.

Denton, D. Keith. "Better decisions with less information." *Industrial Management,* (July-August 2001): 21-25.

Dixon, Nancy. "The neglected receiver of knowledge sharing." *Ivey Business Journal* (March-April 2002): 35-40

Dukart, James R. "Content categorization: Making sense of information overload." *E-Doc,* (January-February 2002): 24.

Erven, Bernard L. "Creative Problem Solving" *The Five Functions of Management.* n.d. <http://www.ag.ohio-state.edu/~mgtexcel/function.html> (10 November 2002).

Ferris, Nancy. "Knowledge is power, Really." *Government Executive,* (June 1999): 63-64.

Garrett, Anthony R. "Information Superiority and the future of mission orders." *Military Review* (November-December 1999): 61-69.

Goldsborough, Reid. "Breaking the information logjam." *Consumer Research Magazine,* (June 2002): 30.

Headquarters, Department of the Army, *Field Manual No 3.0 Operations*, Washington, D.C: Government Printing Office, 2001.

Headquarters, Department of the Army. Field Manual 6.0, Command and Control DRAG, Washington, DC: GPO, TBP.

Hodge, John. "Enlightened Knowledge Management." *Insurance and Technology*, (June 1999): 59-60

Johnson, Stuart E. and Alexander H. Levis, ed. *Science of Command and Control: Coping with Uncertainty*. Washington, DC: AFCEA International Press, 1988.

Kennedy, Shirley Duglin. "Finding a cure for information anxiety." *Information Today*, (May 2001): 40-41

Klien, Gary, *Sources of Power , How People Make Decisions*, Cambridge, MA: Massachusetts Institute of Technology Press, 1998.

Lawlor, Maryann. "Information plus context equals knowledge." *Signal*, (February 2002): 37-40.

Meltzer, Morton F, *Information: the ultimate management resource*. New York: AMACOM, 1981.

Preiss, Kenneth J. "A two-stage process for eliciting and prioritizing critical knowledge." *Journal of Knowledge Management* (2000): 328-36.

Ringle, Bill. "What every business manager should know about knowledge management". *The Canadian Manager* (Summer 2001): 11-27.

Scriven, George P. *The Service of Information, United States Army*. Washington D.C.: Government Printing Office, 1915.

Strassman, Paul A. *The Politics of Information Management – Policy guidelines*. New Canaan, CT: The Information Economics Press, 1995.

Sullivan, Gordon R. *America's Army into the 21st Century*. Hollis, NH: Puritan Press, 1994.

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations*. 6th ed. Chicago: University of Chicago Press, 1996.

Van Creveld, Martin. *Technology and War- From 2000 B.C. to the present*. New York: The Free Press, 1989

Wang, Charles, B. *Techno Vision, the executive's survival guide to understanding and managing information technology*. New York, NY: McGraw Hill, Inc., 1994

Wainwright, Christopher. "Knowledge Management: Aspects of Knowledge." *Management Services*, (November 2001): 16-19.

Zand, Dale E. *Information, Organization, and Power – Effective Management in the Knowledge Society*. New York: McGraw-Hill Book Company, 1981.